Grover's Algorithm Applied to Quantum Cryptography

Z. Sakhi[1], A. Tragha[1], R. Kabil[1], M. Bennai[2]
[1]Laboratory of Information Technology and Modelisation
[2]LPMC, Quantum Physics and Applications Group
[1,2] Ben M'sik Faculty of Sciences
Hassan II-Mohamedia University, PO box 7955
Casablanca, Morocco
{zb.sakhi, relkabil, atragha, mdbennai}@yahoo.fr

ABSTRACT: *We are interested in some applications of a new quantum algorithm in the case of quantum cryptography. We have analyzed in particular Grover algorithm and its implementation in the case of many qubits system. Some features of quantum cryptography are also presented and quantum cryptographic protocol, especially, Quantum Secret-Sharing protocol based on Grover's algorithm is studied.*

Keywords: Qubit, Quantum Cryptography, Grover Algorithm

Received: 12 June 2012, Revised 25 July 2012, Accepted 4 August 2012

1. Introduction

Recently, quantum information has emerged as a new information science introducing simultaneously quantum physics, informatics and electronic. The principal feature of quantum computing is the application of quantum mechanics principles in information processing [1]. Information can, then, be encoded in a superposition of states of a quantum objects like: photons, atoms, or ions. This superposed state was called a qubit. One must signal here that this development was justified, on the other hand, by the increasing miniaturization of electronic components and circuits, leading to quantum effects at nanometer scale.

More recently, a renewed interest in quantum information was seen, since the seminal work of Shor [2] and Grover [3] on quantum algorithms. This makes possible to solve many problems which can't be reached in classical computing, especially in cryptography. Recall that quantum cryptography is an increasing research field and presents a great potential for technological applications, in particular for security systems. The first quantum cryptographic protocol developed was called BB84 following the first letters in the name of the authors Bennett and Brassard in 1984 [4].

In the last few years, Grover algorithm has showed an increasing capacity to solve many problems and was applied in many contexts in particular in quantum cryptography [5]. One of the principal properties of states used in quantum information context is the entanglement, and many variants of entangled states were studied in quantum cryptography like GHZ-states [6] or W-states [7]. Some experimental realizations were also obtained [8]. The case of four qubits is very special and the four qubits systems was studied by many authors and in different context [9].

In this work, we present some cryptographic applications of quantum algorithm in the case of many qubits system. We recall first, in the next section, some basic concept of quantum cryptography. Some features of Grover algorithm and Quantum secret-sharing protocol based on Grover's algorithm are presented in section 3. We consider especially the case of many qubits system, and show specially that Grover algorithm allows us to obtain a good results in the context of quantum cryptography.

2. Quantum Key Distributiion

2.1 Quantum cryptography

Cryptographic protocol often introduces cryptographic keys. Note that the security of most modern cryptographic systems was based on mathematical complexity and the extremely long time needed to break the protocol. Quantum Cryptography offers unconditionally secure communication based on quantum laws.

Quantum cryptography or Quantum Key Distribution (QKD) [4] is a theory for sharing secret keys, whose security is based essentially on exploiting the laws of quantum physics. It allows the users to detect eavesdropping easily.

Recall that the current classical cryptographic technologies, such as RSA and others are based on factorization. It was recently shown that this problem could efficiently be solved using Shor's algorithm [2]. This breaking would have very important implications for electronic privacy and security.

Note that the main goal of quantum cryptography is only to produce and distribute a key. This key can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel. Quantum key distribution has an important and unique properly; it is the ability of the two communicating users (traditionally referred to as Alice and Bob) to detect the presence of any third party (referred to as Eve) trying to gain knowledge of the key. A third party trying to eavesdrop on the key must in some way measure it, thus introducing detectable anomalies. By using quantum entanglement and transmitting information in quantum states over a quantum channel (such as an optical fiber), a communication system can be implemented which detects eavesdropping.

2.2 BB84 Protocol

We shall present here a survey of the most known QKD protocols; the BB84;

To illustrate the BB84 protocol, suppose Alice has a source of photons and suppose that the only degree of freedom considered is polarization. Alice and Bob can use their polarizers and agree to use either the Horizontal/Vertical (+) basis, or the complementary basis of linear polarizations i.e. +45/-45 (×).

One can code the bits as following:

$$|H\rangle \quad \text{codes for} \quad 0_+$$

$$|V\rangle \quad \text{codes for} \quad 1_+$$

$$|+45\rangle \quad \text{codes for} \quad 0_\times$$

$$|+45\rangle \quad \text{codes for} \quad 1_\times$$

The QKD protocols can be summarized in the following steps:

1. Alice can prepare a photon in one of the four states above and sends it to Bob on the quantum channel. Bob measures it in either the + or the × basis. After repetition of this step N times, Alice and Bob can obtain a list of N pairs (bit, basis).

2. Alice and Bob use a classical channel to communicate their results and compare the "*basis*" value of each item and discard those cases where they have used different bases. At its end, Alice and Bob have a list of bits, with the promise that for each of them Alice's coding matched Bob's measurement (the raw key).

3. Alice and Bob now announce a random sequences of the bits of their raw keys and calculate the error rate in the quantum channel, consequently, Eve's information.

In the case of absence of errors, the raw key is identical for Alice and Bob and Eve has no information: in this case, the raw key is already the secret key.

If there are errors however, Alice and Bob have to eliminate the information that Eve could have obtained. At the end of this processing, Alice and Bob share either a truly secret key or nothing at all. In the next section, we show how Grover can be used in the context of quantum cryptography.

3. Quantum Cryptography Based on Grover's Algorithm

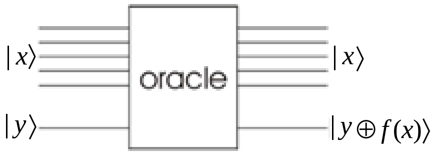
3.1 Grover's algorithm

In order to construct an adequate quantum algorithm, one has to introduce quantum logical gates similar to the classical ones. The most known quantum gates are: Hadamard and CNOT gates. The first one, which is used in the context of Grover algorithm, is a one qubit gate. This gate is very important because it allows as constructing a superposed states from individual qubits. In matrix representation, the Hadamard gate, is a one-qubit rotation, mapping the qubit-basis states $|1\rangle$ and $|0\rangle$ to two superposition states with equal weight of the computational basis states $|1\rangle$ and $|0\rangle$. This corresponds to the transformation matrix given by:

$$H_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \text{ in } \{|0\rangle \text{ and } |1\rangle\} \text{ basis.}$$

In the following, we will recall the essential feature of the Grover algorithm. Suppose we have an unstructured database with N elements which are numbered from 0 to N-1, and the elements are not ordered. Classically, we would test each element at a time, until we get the one searched for. In Grover's algorithm, only $O(\sqrt{N})$ trials are needed [3]. Grover's algorithm has two registers: n qubits in the first one and one qubit in the second.

The first step is to create a superposition of all 2n computational basis states. This is achieved by initializing the first register in the state and applying the operator H_n, where H is the Hadamard gate. Then we define a function f which recognizes the solution as: $f : \{0, ..., N-1\} \rightarrow \{0, 1\}$, f (k) = 1 if k is the searched element, f = 0 otherwise. Note that the function f is also known as an oracle and can be defined as:



Thus, we can resume the Grover algorithm as consisting of the following steps:

1. Consider an initial state: $|0\rangle^{\otimes n}$,
2. We apply the Hadamard gate on the first n qubits to get a uniform superposition of all possible arguments,
3. Apply the oracle f. Note that the information on f are included in the $(n+1)^{th}$ qubit,
4. Apply against the Hadamard gate,
5. Do an observation.

Note that, in this algorithm, we have a succession of a one Grover iteration operator (G) and the states of the first register correspond to the first iteration. In the next section, we show how this algorithm is applied in many qubits system and how it's used in quantum cryptography.

More recently, some research has been focused on another quantum cryptographic protocols: the quantum secret sharing (QSS) originally considered by Hillery *et al.*[10].

In the following, we review a particular QSS Hsu [5] protocol, based on Grover's algorithm. An example of quantum secret sharing scheme using Grover's search algorithm for a two qubits system will be considered. The hope is to generalize this work, later, to other entangled states like W-states or EPR-states.

3.3 Quantum secret-sharing protocol based on Grover's algorithm

In this section, we present one of the most interesting quantum cryptographic protocol: the Hsu QSS protocol, especially in two qubits case. For this purpose, we suppose that the searched state is $| w\rangle$, where w can be either 00, 01, 10 or 11. The initial state is a tensor product of each individual state and is noted $| S_i \rangle$. Each qubits in the state $| S_i \rangle$can be in one of the following states:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle); \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle); \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle); \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$$

Thus, we have a 16 possible states (i = 1, 2, … 16). Consider, for example, the state

$$| S_1\rangle = \left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle);\right]^{\otimes 2}$$

The protocol use different states: *carried* state, en*coded* state and *key* state. The carried state is a state randomly chosen from the states $| S_i \rangle$. Encoded state is obtained after applied the unitary transformation on carried state S_1: $| S_1\rangle_w = U_w\,|S_1\rangle$, where $U_w = I - 2\,| w\rangle\langle w|$ and I is the unit operator and w is the encoded qubits such as 00, 01, 10 and 11.

The key state is obtained after applied the operator of decoding $U_{s_1} = I - 2\,| S_1\rangle\langle S_1|$ on the coded state, the key state is obtained:

$-U_{s_1}\,| S_1\rangle_w = a\,| w\rangle$; where a is some phase term and w can be 00, 01, 10, or 11.

Suppose now that the message is encoded in the state $| 10\rangle$.

Next, we apply the encoding operator on $| S_1 \rangle$. We can obtain then the encoded state $| S_1 \rangle_{10}$:

$$| S_1\rangle_{10} = U_{10}\,|S_1\rangle = [I - 2\,| 10\rangle\langle 10|]\left[\frac{1}{2}\left(| 00\rangle + |01\rangle + |10\rangle + |11\rangle\right)\right]$$

$$= \frac{1}{2}\left(| 00\rangle + |01\rangle + |10\rangle + |11\rangle\right)$$

To obtain the key, one must then apply the decoding operator:

$$-U_s = 2|\,S_1\rangle\langle S_1| - 1$$

on the encoded state $| S_1 \rangle_{10}$. This allows as obtaining the key:

$$-U_{s_1}|S_1\rangle_{10} = [2|\,S_1\rangle\langle S_1| - I]\left[\frac{1}{2}\left(| 00\rangle + |01\rangle + |10\rangle + |11\rangle\right)\right] = |10\rangle$$

This protocol was first introduced by Hsu [4], and can be represented as:

$$| S_i\rangle \xrightarrow{U_w} | S_i\rangle \xrightarrow{-U_{s_i}} | w\rangle$$

where i = 1,……,16.

Finally, we summarize the "*Hsu*" protocol in the following steps:

Step 1: Alice randomly prepares some carrier state $| S_i\rangle$. Then she applies an encoding operation U_w on $| S_i \rangle$, so as to obtain an encoded state $| S_i \rangle_w = U_w\,| S_i \rangle$.

Step 2: Alice sends one of the two qubits of the encoded state to Bob and the other qubit to Charlie respectively. After Bob and Charlie receive their qubits, they announce this fact publicly.

Step 3: Alice has to confirm that each agent has actually received the qubit via classical communication.

Step 4: Alice announces her initial state $|S_i\rangle$ in public.

Step 5: Only when Bob and Charlie combine their qubits and perform $-U_{s_i}$ on these two qubits can they both determine the marked state $|w\rangle$ with certainty.

4. Conclusion

In this paper, we have presented some applications of quantum algorithm in the quantum information processing system. We have analyzed, in particular, the basic concept of Grover algorithm and its implementation in the case of many qubits system. Some features of quantum cryptography and Quantum secret-sharing protocol based on Grover's algorithm were also presented. In particular QSS Hsu protocol using Grover's search algorithm for a two qubits system was studied. This work is in it's beginning and must be improved to get a more protected protocol for some communication applications.

References

[1] Nielsen, M. A., Chuang, I. L.(2000). *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge)

[2] Shor, P. W. (1994). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *In*: Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, edited by S. Goldwasser, p. 124, Los Alamitos, CA, *IEEE Computer Society*.

[3] Grover, L. K. (1997). Quantum Mechanics Helps in Searching for a Needle in a Haystack, *Phys. Rev. Lett*. 79, 325.

[4] Bennett, C., Brassard, G. (1984). cryptography: public key distribution and coin tossing, *In*: Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing (Bangalore, India 1984) p.175.

[5] Li-Yi-Hsu. (2003). Quantum secret-sharing protocol based on Grover's algorithm, *Phys. Rev. A* 68, 022306.

[6] Saber Bagherinezhad, Vahid Karimipour. (2003). Quantum secret sharing based on reusable GHZ states as secure carriers, *Physical Rev. A*, 67, 044302.

[7] DONG Li, XIU Xiao-Ming, GAO Ya-Jun, CHI Feng. (2008). Quantum Secure Direct Communication Using W State, Commun. Theor. Phys. (Beijing, China) 49, p. 1495–1498.

[8] Yu-Ao Chen, An-Ning Zhang, Zhi Zhao, Xiao-Qi Zhou, Chao-Yang Lu, Cheng-Zhi Peng, Tao Yang, Jian-Wei Pan. (2005). Experimental Quantum Secret Sharing and Third-Man Quantum Cryptography, *Phys. Rev. Lett*. 95, 200502.

[9] Sakhi, Z., Tragha, A., Kabil, R., Bennai, M. (2011). Grover Algorithm Applied to Four Qubits System, *Computer and Information Science*, 4 (3).

[10] Hillery, M., Buzek, V., Berthiaume, A. (1999). Quantum secret sharing, Phys. Rev. A 59, 1829-1834.